
Bezpieczeństwo tożsamości i danych w projektach Web

*Jonathan LeBlanc
Tim Messerschmidt*

przekład: Marek Włodarz

APN Promise
Warszawa 2016

O'REILLY®

Spis treści

<i>Przedmowa</i>	<i>vii</i>
1 Wprowadzenie	1
Problemy z obecnymi modelami zabezpieczeń.....	1
Kiepskie hasła.....	3
Bezpieczeństwo kontra użyteczność.....	4
Niewłaściwe szyfrowanie danych.....	5
Najsłabsze ogniwo: ludzie.....	5
Pojedyncze logowanie.....	7
Pojęcie entropii a bezpieczeństwo haseł.....	7
Entropia losowo generowanych haseł.....	8
Entropia haseł tworzonych przez ludzi.....	9
Nazwa użytkownika i hasło – analiza.....	12
Zabezpieczanie istniejących standardów dla ochrony tożsamości.....	12
Dobre i złe algorytmy zabezpieczeń.....	13
Jakie dane powinny być chronione?.....	14
Mechanizmy odzyskiwania kont a socjotechnika.....	14
Problem pytań bezpieczeństwa.....	15
Co dalej?.....	16
2 Hasła: szyfrowanie, haszowanie i solenie	17
Dane w spoczynku kontra dane w ruchu.....	17
Dane w spoczynku.....	18
Dane w ruchu.....	19
Wektory ataku na hasła.....	20
Ataki siłowe.....	21
Tworzenie CAPTCHA przy użyciu reCAPTCHA.....	22
Ataki słownikowe.....	28
Odwrotne tabele wyszukiwania.....	29
Tęczowe tabele.....	30
Solenie.....	32
Generowanie losowej soli.....	33
Ponowne użycie soli.....	34
Długość soli.....	34
Gdzie przechowywać sól.....	34
Pieprz.....	35
Wybieranie właściwej funkcji haszującej dla haseł.....	36

bcrypt	36
PBKDF2	37
script	39
Weryfikowanie hasła względem wartości haszowanej	40
Rozciąganie kluczy	41
Ponowne obliczanie skrótów	42
Co dalej?	42
3 Podstawy bezpieczeństwa tożsamości	43
Istota koncepcji różnych typów tożsamości	43
Tożsamość społecznościowa	44
Tożsamość zweryfikowana	44
Tożsamość minimalna	45
Ulepszanie środowiska użytkownika dzięki wykorzystaniu tożsamości	45
Wprowadzenie do koncepcji stref zaufanych	46
Odcisk palca przeglądarki	47
Konfiguracje bardziej odporne na identyfikowanie przeglądarek	48
Identyfikowalne informacje przeglądarki	49
Przechwytywanie szczegółów przeglądarki	50
Śledzenie oparte na lokalizacji	52
Odcisk palca urządzenia (telefon / tablet)	54
Odcisk palca urządzenia (urządzenia sparowane przez Bluetooth)	55
Implementowanie tożsamości	56
4 Zabezpieczanie logowania przy użyciu OAuth 2 i OpenID Connect	57
Różnica pomiędzy uwierzytelnieniem a autoryzacją	57
Uwierzytelnianie	57
Autoryzacja	58
Czym są OAuth i OpenID Connect?	58
Wprowadzenie do OAuth 2.0	61
Obsługa autoryzacji przy użyciu OAuth 2.0	63
Korzystanie z tokenu Bearer	64
Autoryzacja i uwierzytelnianie przy użyciu OpenID Connect	65
Różnice uwarunkowań zabezpieczeń pomiędzy OAuth 2 i OAuth 1.0a	66
Budowanie serwera OAuth 2.0	67
Tworzenie aplikacji Express	67
Konfigurowanie bazy danych naszego serwera	68
Generowanie kodów autoryzacyjnych i tokenów	68
Punkt końcowy autoryzacji	71
Obsługa czasu życia tokenu	75
Obsługa żądań zasobów	78
Korzystanie z tokenów odświeżania	81
Obsługa błędów	83

Dodawanie funkcjonalności OpenID Connect do serwera.	87
Schemat ID Token	88
Modyfikowanie punktu końcowego autoryzacji	89
Dostosowywanie punktu końcowego Token	90
Punkt końcowy UserInfo	92
Zarządzanie sesją przy użyciu OpenID Connect.	93
Budowanie klienta OAuth 2.	93
Używanie kodów autoryzacyjnych	93
Autoryzacja przy użyciu poświadczeń właściciela zasobu lub poświadczeń klienta	96
Dodawanie funkcjonalności OpenID Connect do klienta.	98
Przepływ podstawowy OpenID Connect.	98
Poza OAuth 2.0 i OpenID Connect	100
5 Alternatywne metody identyfikacji	101
Identyfikowanie urządzeń i przeglądarek	101
Uwierzytelnianie dwuskładnikowe oraz n-składnikowe	102
Uwierzytelnianie n-składnikowe	102
Hasła jednorazowe	103
Implementowanie dwuskładnikowego uwierzytelniania przy użyciu Authy	106
Biometria jako uwierzytelnienie zamiast hasła	112
Jak oceniać skuteczność biometrii.	113
Rozpoznawanie twarzy	114
Skanowanie siatkówki i tęczówki.	114
Rozpoznawanie naczyń krwionośnych.	115
Przyszłe standardy	115
FIDO Alliance	116
Oz	117
Blockchain.	118
Co dalej?	118
6 Wzmacnianie aplikacji Web.	119
Zabezpieczanie sesji	119
Różne typy sesji	120
Jak Express obsługuje sesje	121
Obsługa XSS	125
Trzy typy ataków XSS	125
Testowanie mechanizmów ochrony przed XSS	126
Podsumowanie	130
Ataki CSRF	131
Obsługa CSRF za pomocą csrf.	131

Wartościowe zasoby dla platformy Node	132
Lusca	132
helmet	133
Node Security Project	134
Inne techniki neutralizacyjne	135
Nasze odkrycia	136
7 Bezpieczeństwo transmisji danych	137
SSL/TLS	137
Typy certyfikatów i urzędów certyfikacji	138
Tworzenie samopodpisanego certyfikatu na potrzeby testów	140
Kryptografia asymetryczna	148
Przypadki zastosowań	148
Przykład implementacji	150
Zalety, wady i zastosowania kryptografii asymetrycznej	157
Kryptografia symetryczna	158
Wektor inicjujący	159
Dopełnienie	159
Tryby działania szyfrów blokowych	161
Korzystanie z AES w trybie szyfrowania CTR	164
Korzystanie z AES w trybie szyfrowania z uwierzytelnieniem GCM	166
Zalety, wady i zastosowania kryptografii symetrycznej	168
A Repozytoria GitHub	169
B Wymagania techniczne i warunki wstępne	171
<i>Słowniczek</i>	<i>179</i>
<i>Indeks</i>	<i>181</i>